UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/810,688	03/29/2004	Nambi Seshadri	1875.3820001	1270

26111 7590 10/10/2008

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
1100 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
GERGISO, TECHANE	
ART UNIT	PAPER NUMBER
2437	
MAIL DATE	DELIVERY MODE
10/10/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/810,688	SESHADRI, NAMBI	
	Examiner	Art Unit	
	TECHANE J. GERGISO	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 May 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24,31-61 and 68-74* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24, 31-61, 68-74* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is a Final Office Action in response to the applicant's communication filed on May 22, 2008.

2. Claims 1-24, 31-61 and 68-74 are pending.

Response to Arguments

3. Applicant's arguments filed on May 22, 2008 have been fully considered but they are not persuasive.

The applicant argues that Yu does not teach or suggest features of "processing a second part of the message with a second level of encryption to produce a second message portion, including selecting the second level of encryption from a group consisting of: (i) no encryption, and (ii) a level of encryption less strong than the first level of encryption" as recited by claim 1 (See applicant's argument filed on may 22, 2008 on page 16, page 18, and 19).

However, the examiner disagrees with the applicant's argument and analysis. Yu discloses a method and a system for partially or selective encryption of audio and video data for various applications. Furthermore, Yu provides a method to select different encryption algorithms from a set of encryption algorithms in order to differently encrypt subsets of the data being encrypted.

The applicant is intending to achieve selective encryption as it is claimed and also argued. However, Yu suggests that selective encryption is generally well known to one of ordinary skill in the art recited as follows:.

(Yu column 11: lines 15-22; column 11: lines 30-47; figure 11: 1110, 1113, 114; figure 12: 1206; 212, 1214,1215):

"It is to be understood for certain kinds of video or audio, for instance military video/audio, it may be required to encrypt the entire video with a strong encryption algorithm to achieve the highest security. When computational time is a significant consideration, scalable and fine granularity scalable (when streaming or real time is required) encryption may be used such that the strongest encryption (that requires the most processing time) can be used on the most sensitive information part while less strong encryption (with less computational complexity) can be used in a less sensitive information part etc. **In general, selective switching of encryption strength is known. For example, see U.S. Pat. No. 5,323,464, which is hereby incorporated by reference, and which discloses a method for selecting between two different types of encryption, specifically a weak symmetric cryptographic algorithm CDM (commercial data masking) and a strong encryption algorithm DEA (Data Encryption Algorithm) of encryption algorithms for use on different data**."

Therefore, the applicant's invention as it is recited in claim 1, is directed to a selective encryption by partitioning a message into a first part and a second part and encrypting the first part with the first encryption level and, not encrypting or encrypting the second part with another encryption level. These claimed features are anticipated by Yu as it is disclosed an recited above. Therefore, for the above reasons, the applicant's argument is not persuasive to overcome Yu and place independent claim 1 in condition for allowance. The applicant has a similar argument

regarding independent claims 31, 38 and 68 as in claim 1. Again with the same rational and reason give above for claim 1, the applicant's argument is not persuasive to overcome Yu and place independent claims 31, 38 and 68 in condition for allowance. Dependent claims 2-24, 32-37, 39-62, and 69-74 depending directly or indirectly from their corresponding independent claims are also not placed in condition for allowance based on their dependency.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-4, 31-41 and 68-74 are rejected under 35 U.S.C. 102(e) as being anticipated by Yu (US Pat. No.: 7,167,560).

As per claim 1:

YU discloses a method of securely transmitting a message to a receiving device, comprising the steps of:

(a) encrypting a first part of said message with a first level of encryption to produce a first message portion *(column 3: lines 33-37; partitioning the media into cloak data and non-cloak data; and encrypting the cloak data such that less than all of*

said stream-formatted media is encrypted; column 5: lines 18-35; column 5: lines 60-67; column 6: lines 7-18);

(b) processing a second part of said message with a second level of encryption to produce a second message portion, with the second level of encryption selected from the group consisting of:

(i) no encryption *(column 3: lines 33-37; column 5: lines 18-35; column 5: lines 60-67; column 6: lines 7-18; Figure 11: 1110; Figure 12: 212; non-cloak)*; and

(ii) a level of encryption less strong than said first level of encryption *(column 7: lines 33-50; column 7: lines 63-67; column 8: lines 13-25; column 9: lines 1-14; column 9: lines 22-45; column 9: lines 54-67; column 10: lines 1-10; column 11: lines 15-22; column 11: lines 30-47; figure 11: 1110, 1113, 114; figure 12: 1206; 212, 1214,1215)*;

(c) transmitting said first and second message portions over at least one transmission channel *(figure 1: output)*; and

(e) providing an output at the receiving device including at least one of: at least part of said data from said first part of said message and at least part of said data from said second part of said message *(column 7: lines 33-50; column 7: lines 63-67; column 8: lines 13-25; column 9: lines 1-14; column 9: lines 22-45; column 9: lines 54-67; column 10: lines 1-10; column 11: lines 15-22; column 11: lines 30-47; figure 11: 1110, 1113, 114; figure 12: 1206; 212, 1214,1215)*.

As per claim 31:

YU discloses a method of securely transmitting a message to a receiving device, comprising the steps of:

(a) selecting a first encryption algorithm (*figure 11: 1110, 1113, 114; figure 12: 1206; 212, 1214,1215)*;

(b) encrypting a first part of said message with said first encryption algorithm to produce a first data set *(column 3: lines 33-37; partitioning the media into cloak data and non-cloak data; and encrypting the cloak data such that less than all of said stream-formatted media is encrypted; column 5: lines 18-35; column 5: lines 60-67; column 6: lines 7-18)*;

(c) selecting a second encryption algorithm from the group consisting of:

(i) no encryption *(column 3: lines 33-37; column 5: lines 18-35; column 5: lines 60-67; column 6: lines 7-18)*, and

(ii) those algorithms requiring less processing overhead than required by said first encryption algorithm *(column 7: lines 33-50; column 7: lines 63-67; column 8: lines 13-25; column 9: lines 1-14; column 9: lines 22-45; column 9: lines 54-67; column 10: lines 1-10; column 11: lines 15-22; column 11: lines 30-47; figure 11: 1110, 1113, 114; figure 12: 1206; 212, 1214,1215)*;

(d) producing from a second part of said message a second data set incorporating encryption to an extent determined by said step of selecting a second encryption algorithm *(column 7: lines 33-50; column 7: lines 63-67; column 8: lines 13-25;*

column 9: lines 1-14; column 9: lines 22-45; column 9: lines 54-67; column 10: lines 1-10; column 11: lines 15-22; column 11: lines 30-47; figure 11: 1110, 1113, 114; figure 12: 1206; 212, 1214,1215);

(e) generating signals that transmit to a receiving device, over at least one transmission channel, said first and second data sets and information sufficient for said receiving device to determine the type of encryption applied to at least one of said first and second data sets respectively *(column 7: lines 33-50; column 7: lines 63-67; column 8: lines 13-25; column 9: lines 1-14; column 9: lines 22-45; column 9: lines 54-67; column 10: lines 1-10; column 11: lines 15-22; column 11: lines 30-47; figure 11: 1110, 1113, 114; figure 12: 1206; 212, 1214,1215)*; and

(f) providing an output at the receiving device including at least one of: at least part of said data from said first part of said message and at least part of said data from said second part of said message *(column 7: lines 33-50; column 7: lines 63-67; column 8: lines 13-25; column 9: lines 1-14; column 9: lines 22-45; column 9: lines 54-67; column 10: lines 1-10; column 11: lines 15-22; column 11: lines 30-47; figure 11: 1110, 1113, 114; figure 12: 1206; 212, 1214,1215)*.

As per claims 2 and 32:

YU discloses a method, including the step of: determining whether at least part of said first message portion should be decrypted upon receipt, and if so decrypting at least part of said first message portion to produce data from said first part of said message (column 7: lines 45-60; column 9: lines 1-10).

As per claims 3 and 33:

YU discloses a method, including the step of: determining whether at least part of said second message portion should be decrypted upon receipt, and if so decrypting at least part of said second message portion to produce data from said second part of said message (column 7: lines 45-60; column 9: lines 1-10).

As per claim 4:

YU discloses a method, wherein said first part of said message is encrypted with an asymmetric algorithm and said first message portion is decrypted on receipt and provided to the receiving device (column 5: lines 18-35).

As per claim 34:

Yu discloses a method, wherein said information sufficient for said receiving device to determine the type of encryption applied to at least one of said first and second data sets respectively comprises header information identifying those portions of the transmitted signal to which the first and second encryption algorithms were applied (column 8: lines 45-60).

As per claim 35:

Yu discloses a method, wherein transmitting to the receiving device information defining at least one of the first and second encryption algorithms (column 7: lines 45-60; column 9: lines 1-10).

As per claim 36:

Yu discloses a method, wherein first and second data sets are divided into packets and a plurality of said packets are transmitted in frames incorporating said information sufficient for said receiving device to determine the type of encryption applied to at least one of said first and second data sets respectively (Figure 8B, 8C).

As per claim 37:

Yu discloses a method, wherein at least one said frame is transmitted with a flag bit to indicate a level of encryption of the data (Figure 8B).

As per claim 38:

YU discloses a system for securely transmitting a message to a receiving device, comprising:

(a) first processing means for encrypting a first part of said message with a first level of encryption to produce a first message portion *(column 3: lines 33-37; partitioning the media into cloak data and non-cloak data; and encrypting the cloak data such that less than all of said stream-formatted media is encrypted; column 5: lines 18-35; column 5: lines 60-67; column 6: lines 7-18; figure 11: 1110, 1113, 114; figure 12: 1206; 212, 1214,1215)*;

(b) second processing means for encrypting a second part of said message to produce a second message portion, using a second level of encryption from the group consisting of:

(i) no encryption *(column 3: lines 33-37; column 5: lines 18-35; column 5: lines 60-67; column 6: lines 7-18)*, and

(ii) a level of encryption less strong than said first level of encryption *(column 7: lines 33-50; column 7: lines 63-67; column 8: lines 13-25; column 9: lines 1-14; column 9: lines 22-45; column 9: lines 54-67; column 10: lines 1-10; column 11: lines 15-22; column 11: lines 30-47; figure 11: 1110, 1113, 114; figure 12: 1206; 212, 1214,1215)*;

(c) transmitting means operably connected to said first processing means and said second processing means for transmitting said first and second message portions over at least one transmission channel *(column 7: lines 33-50; column 7: lines 63-67; column 8: lines 13-25; column 9: lines 1-14; column 9: lines 22-45; column 9: lines 54-67; column 10: lines 1-10; column 11: lines 15-22; column 11: lines 30-47; figure 11: 1110, 1113, 114; figure 12: 1206; 212, 1214,1215)*; and

(e) output means connected to receive information from said transmission channel for providing an output at the receiving device including at least one of: at least part of said data from said first part of said message and at least part of said data from said second part of said message *(column 7: lines 33-50; column 7: lines 63-67; column 8: lines 13-25; column 9: lines 1-14; column 9: lines 22-45; column 9:*

lines 54-67; column 10: lines 1-10; column 11: lines 15-22; column 11: lines 30-47; figure 11: 1110, 1113, 114; figure 12: 1206; 212, 1214,1215).

As per claim 39:

Yu discloses a system comprising means for determining whether at least part of said first message portion should be decrypted upon receipt, and if so decrypting at least part of said first message portion to produce data from said first part of said message (column 7: lines 45-60; column 9: lines 1-10)..

As per claim 40:

Yu discloses a system comprising means for determining whether at least part of said second message portion should be decrypted upon receipt, and if so decrypting at least part of said second message portion to produce data from said second part of said message (column 7: lines 45-60; column 9: lines 1-10).

AS per claim 41:

Yu discloses a system comprising said first processing means encrypts said first part of said message with an asymmetric algorithm and said output means further includes means for decrypting said first message portion on receipt for use by the receiving device (column 5: lines 18-35).

As per claim 68:

YU discloses a system for securely transmitting a message to a receiving device using a first encryption algorithm and a second encryption algorithm selected from the group consisting of: (i) no encryption, and (ii) those algorithms requiring less processing overhead than required by said first encryption algorithm, comprising:

(a) first processing means for encrypting a first part of said message with said first encryption algorithm to produce a first data set *(column 3: lines 33-37; partitioning the media into cloak data and non-cloak data; and encrypting the cloak data such that less than all of said stream-formatted media is encrypted; column 5: lines 18-35; column 5: lines 60-67; column 6: lines 7-18; figure 11: 1110, 1113, 114; figure 12: 1206; 212, 1214,1215)*;

(b) second processing means for producing from a second part of said message a second data set incorporating encryption to an extent determined by said second encryption algorithm *((column 3: lines 33-37; column 5: lines 18-35; column 5: lines 60-67; column 6: lines 7-18; column 7: lines 33-50; column 7: lines 63-67; column 8: lines 13-25; column 9: lines 1-14; column 9: lines 22-45; column 9: lines 54-67; column 10: lines 1-10; column 11: lines 15-22; column 11: lines 30-47; figure 11: 1110, 1113, 114; figure 12: 1206; 212, 1214,1215)*;

(c) transmission means for generating signals for transmission to a receiving device over at least one transmission channel, said signals representing said first and second data sets and information sufficient for said receiving device to determine a type of encryption applied to at least one of said first and second data sets respectively

(column 7: lines 33-50; column 7: lines 63-67; column 8: lines 13-25; column 9: lines 1-14; column 9: lines 22-45; column 9: lines 54-67; column 10: lines 1-10; column 11: lines 15-22; column 11: lines 30-47; figure 11: 1110, 1113, 114; figure 12: 1206; 212, 1214,1215); and

(d) output means for providing an output at the receiving device including at least one of: at least part of said data from said first part of said message and at least part of said data from said second part of said message *(column 7: lines 33-50; column 7: lines 63-67; column 8: lines 13-25; column 9: lines 1-14; column 9: lines 22-45; column 9: lines 54-67; column 10: lines 1-10; column 11: lines 15-22; column 11: lines 30-47; figure 11: 1110, 1113, 114; figure 12: 1206; 212, 1214,1215)*.

As per claim 69:

YU discloses a system wherein the output means further includes means for decrypting at least part of said first data set to produce data from said first part of said message (column 7: lines 45-60; column 9: lines 1-10).

As per claim 70:

YU discloses a system wherein the output means further includes means for decrypting at least part of said second data set to produce data from said second part of said message (column 7: lines 45-60; column 9: lines 1-10).

As per claim 71:

YU discloses a system wherein said transmission means further comprises means for generating and transmitting header information identifying those portions of the transmitted signal to which the first and second encryption algorithms were applied (column 5: lines 18-35).

As per claim 72:

YU discloses a system wherein said transmission means further comprises means for transmitting to the receiving device information identifying at least one of the first and second encryption algorithms.

As per claim 73:

YU discloses a system wherein said transmission means further comprises framing means for dividing said first and second data sets into packets and transmitting said packets in frames incorporating said information sufficient for said receiving device to determine the type of encryption applied to at least one of said first and second data sets respectively *(column 7: lines 33-50; column 7: lines 63-67; column 8: lines 13-25; column 9: lines 1-14; column 9: lines 22-45; column 9: lines 54-67; column 10: lines 1-10; column 11: lines 15-22; column 11: lines 30-47)*.

As per claim 74:

YU discloses a system wherein at least one said frame is transmitted with a flag bit to indicate a level of encryption of the data (figure 8).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 5- 24 and 42-53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yu (US Pat. No.: 7,167,560) in view of Nag (US Pat. No.: 7,266,683)

As per claim 5:

Yu does not explicitly disclose first part of said message is encrypted for transmission, said second part of said message is not encrypted for transmission, and neither of said first and second message portions are decrypted upon receipt. Nag, in analogous art, however, discloses first part of said message is encrypted for transmission, said second part of said message is not encrypted for transmission, and neither of said first and second message portions are decrypted upon receipt (column 6: lines 39-46). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Yu to include first part of said message is encrypted for transmission, said second part of said message is not encrypted for transmission, and neither of said first and second message portions are decrypted upon receipt. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide an apparatus and methods

for multiplexing and selectively encrypting application flows over a pre-allocated bandwidth reservation protocol session as suggested by Nag in (column 2: lines 35-45).

As per claim 6:

Yu discloses a method, wherein said first part of said message is encrypted for transmission, said second part of said message is encrypted for transmission with said second level of encryption less strong than said first level of encryption, and said second message portion is decrypted upon receipt *(column 7: lines 33-50; column 7: lines 63-67; column 8: lines 13-25; column 9: lines 1-14; column 9: lines 22-45; column 9: lines 54-67; column 10: lines 1-10; column 11: lines 15-22; column 11: lines 30-47; figure 11: 1110, 1113, 114; figure 12: 1206; 212, 1214,1215).*

As per claim 7:

Yu discloses a method, wherein said first message portion is decrypted upon receipt *(column 7: lines 33-50; lines 63-67; column 8: lines 13-25; column 9: lines 1-14; lines 22-45; lines 54-67; column 10: lines 1-10; column 11: lines 15-22; lines 30-47).*

As per claim 8:

Yu discloses a method, wherein said first part of said message is encrypted for transmission, said second part of said message is not encrypted for transmission, and part of said first message portion is decrypted upon receipt (column 6: lines 39-46).

As per claim 9:

Yu discloses a method, wherein said first part of said message is encrypted for transmission with said first level of encryption, said second part of said message is encrypted for transmission with said second level of encryption less strong than said first level, and part of said first message portion is decrypted upon receipt and provided to the receiving device *(column 7: lines 33-50; column 7: lines 63-67; column 8: lines 13-25; column 9: lines 1-14; column 9: lines 22-45; column 9: lines 54-67; column 10: lines 1-10; column 11: lines 15-22; column 11: lines 30-47; figure 11: 1110, 1113, 114; figure 12: 1206; 212, 1214,1215).*

As per claim 10:

Yu discloses a method, wherein said second message portion is decrypted upon receipt and provided to the receiving device *(column 7: lines 33-50; lines 63-67; column 8: lines 13-25; column 9: lines 1-14;lines 22-45; lines 54-67; column 10: lines 1-10; column 11: lines 15-22; lines 30-47).*

As per claim 11:

Yu discloses a method, wherein said first message portion and said second message portion are divided into frames and in step (c) frames of said first message portion and frames of said second message portion are alternately transmitted over said at least one transmission channel (figure 5: frame #).

As per claim 12:

Nag discloses a method, wherein said message comprises speech data and said transmission channel comprises a mobile telephone system channel (column 16: lines 35-45).

As per claim 13:

Yu discloses a method, a fraction of the speech data sufficient to prevent understanding of an intercepted message is strongly encrypted and transmitted in said first message portion (column 9: lines 35-50) .

As per claim 14:

Yu discloses a method, a fraction said message includes video telephone data and said video telephone data is at least partially encrypted and is not decrypted upon receipt unless one or more subscribers involved in exchanging the message has agreed to pay for video telephone service (column 7: lines 31-44).

As per claim 15:

Yu discloses a method, encoding said speech data to produce a coded data set Figure 1: encoded bit stream);

in step (a), encrypting and transmitting in said first message portion encoding data useful in decoding said coded data set (Figure 1: 111);

in step (b), selecting and applying said second level of encryption to said coded data set to form said second message portion (Figure 12: 1206);

decrypting said encoding data upon receipt; and using said encoding data to decode said coded data set to obtain said speech data (column 11: lines 5-9).

As per claim 16:

Nag discloses a method, wherein said encoding step is performed with a speech codec (column 4: lines 55-67).

As per claim 17:

Yu discloses a method, wherein said transmitting step includes the step of transmitting information indicating which portions of the transmission are encrypted (figure 3: encrypted, non-encrypted).

As per claim 18:

Yu discloses a method, wherein said first message portion and said second message portion are comprised of a plurality of frames (figure 3: encrypted, non-encrypted).

As per claim 19:

Yu discloses a method, wherein encrypted frames comprise data indicating a level of encryption applied to said encrypted frames (figure 11: 1110).

As per claim 20:

Yu discloses a method, wherein said level indicating data is a frame encryption flag (figure 11: 110).

As per claim 21:

Yu discloses a method, wherein said message comprises video data and said transmission channel comprises a video distribution channel (figure 9).

As per claim 22:

Yu discloses a method, wherein said video distribution channel comprises a cable television distribution channel (figure 9).

As per claim 23:

Yu discloses a method, wherein selecting a plurality of key data elements of said video data containing information needed to properly process and display the video data;

in step (a), encrypting and transmitting in said first message portion said key data elements (Figure 1: 111);

in step (b), selecting and applying said second level of encryption to at least some of said video data not designated as key data elements (Figure 12: 1206);

decrypting said key data elements upon receipt; and using data from said key data elements to process and display said video data (column 11: lines 5-9).

As per claim 24:

Yu discloses a method, wherein said key data elements contain I-signal video information (column 2: lines 40-45).

As per claim 42:

Yu does not explicitly disclose first processing means encrypts said first part of said message for transmission, said second processing means uses no encryption for said second part of said message, and said output means provides said first message portion to the receiving device without decrypting said first message portion, whereby said receiving device can process said second part of said message but cannot interpret said first part of said message. Nag, in analogous art, however, discloses first processing means encrypts said first part of said message for transmission, said second processing means uses no encryption for said second part of said message, and said output means provides said first message portion to the receiving device without decrypting said first message portion, whereby said receiving device can process said second part of said message but cannot interpret said first part of said message (column 6: lines 39-46). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Yu to include first processing means encrypts said first part of said message for transmission, said second processing means uses no encryption for said second part of said message, and said output means provides said first message portion to the receiving device without decrypting said first message portion, whereby said receiving device can process said second part of said message but cannot interpret said first part of said message. This modification would have been obvious because a person

having ordinary skill in the art would have been motivated to do so to provide an apparatus and methods for multiplexing and selectively encrypting application flows over a pre-allocated bandwidth reservation protocol session as suggested by Nag in (column 2: lines 35-45).

As per claim 43:

Yu discloses a system, wherein first processing means encrypts said first part of said message for transmission, said second processing means encrypts said second part of said message with said second level of encryption less strong than said first level of encryption, and said output means comprises means for decrypting said second message portion upon receipt (column 6: lines 39-46).

As per claim 44:

Yu discloses a system, wherein said output means further comprises means for decrypting said first message portion upon receipt *(column 7: lines 33-50; lines 63-67; column 8: lines 13-25; column 9: lines 1-14;lines 22-45; lines 54-67; column 10: lines 1-10; column 11: lines 15-22; lines 30-47)*.

As per claim 45:

Yu discloses a system, wherein said first processing means encrypts said first part of said message, said second processing means applies no encryption to said second part of said message, and said output means includes means for decrypting a first subset of said first message

portion and providing to said receiving device said decrypted first subset of said first message and a second subset of said first message that is not decrypted (column 6: lines 39-46).

As per claim 46:

Yu discloses a system, wherein said first processing means encrypts said first part of said message, said second processing means encrypts said second part of said message with said second level of encryption less strong than said first level, and said output means includes means for decrypting a first subset of said first message portion and providing to said receiving device said decrypted first subset of said first message and a second subset of said first message that is not decrypted *(column 7: lines 33-50; column 7: lines 63-67; column 8: lines 13-25; column 9: lines 1-14; column 9: lines 22-45; column 9: lines 54-67; column 10: lines 1-10; column 11: lines 15-22; column 11: lines 30-47; figure 11: 1110, 1113, 114; figure 12: 1206; 212, 1214,1215).*

As per claim 47:

Yu discloses a system, wherein said output means comprises means for decrypting said second message portion upon receipt and providing a resulting decrypted second message portion to the receiving device *(column 7: lines 33-50; lines 63-67; column 8: lines 13-25; column 9: lines 1-14;lines 22-45; lines 54-67; column 10: lines 1-10; column 11: lines 15-22; lines 30-47).*

As per claim 48:

Yu discloses a system, wherein said transmission means comprises means for dividing said first message portion and said second message portion into frames alternately transmitting frames of said first and second message portions over said at least one transmission channel (figure 5: frame #).

As per claim 49:

Nag discloses a system, wherein said message comprises speech data and said transmission channel comprises a mobile telephone system channel (column 16: lines 35-45).

As per claim 50:

Yu discloses a system, wherein a fraction of the speech data sufficient to prevent understanding of an intercepted message is encrypted and transmitted in said first message portion (column 9: lines 35-50).

As per claim 51:

Yu discloses a system, wherein said message includes video telephone data and said video telephone data is at least partially encrypted and decrypted upon receipt only if one or more subscribers involved in the message exchange is a video telephone service subscriber (column 7: lines 31-44).

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See the notice of reference cited in form PTO-892 for additional prior art.

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Contact Information

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to **Techane J. Gergiso** whose telephone number is **(571) 272-3784** and fax number is **(571) 273-3784**. The examiner can normally be reached on 9:00am - 6:00pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **Emmanuel Moise** can be reached on **(571) 272-3865**. The fax phone number for the organization where this application or proceeding is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/T. J. G./

Examiner, Art Unit 2437

/Emmanuel L. Moise/

Supervisory Patent Examiner, Art Unit 2437